REMARKS

Claims 1-4 and 6-10 are pending in the Application.

Claims 1-4 and 6-10 stand rejected.

I. REJECTIONS UNDER 35 U.S.C. § 101

Claims 4-7 stand rejected under 35 U.S.C. § 101 because the cited claims are directed to a computer program product that is adapted for storage on a computer storage-readable medium. The Examiner believes that the claim language "adaptable" merely suggests limitations or makes limitations optional. In response, Applicants respectfully traverse such an assertion by the Examiner. Nevertheless, in order to move the claims towards being in condition for allowance, Applicants have amended claim 4 to remove the term "adaptable."

II. DOUBLE PATENTING REJECTION

Claims 1, 4 and 8 stand provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 18 (and claim 3) of co-pending Application No. 09/931,550. In response, Applicants respectfully traverse this rejection. However, since the co-pending application is merely pending, Applicants will address this double patenting rejection when either such co-pending application issues or claims 1, 4 and 8 are allowed in this application.

III. REJECTIONS UNDER 35 U.S.C. § 103

Claims 1-4 and 6-10 stand rejected under 35 U.S.C. § 103 as being unpatentable over *Alexander* (U.S. Patent No. 6,188,602), in view of *Grawrock* (U.S. Patent No. 6,678,833). In response, Applicants respectfully traverse these rejections.

The Examiner admits that *Alexander* does not teach using a trusted platform module (TPM) to perform a signature verification of an update to the program.

The Examiner asserts that *Grawrock* teaches a TPM to perform a signature verification of an update to the program. The Examiner then goes on to assert that it would have been obvious to combine *Grawrock* and *Alexander* to arrive at the claimed invention. Applicants respectfully disagree.

The Examiner is respectfully requested to refer to the declaration under 37 C.F.R. §1.132 (the "132 Declaration") by the inventors previously provided. This Declaration is still valid, since the *Grawrock* patent discloses the same technology as the *Grawrock* November 2000 Paper. According to the inventors, *Grawrock* teaches that the verification of the BIOS occurs after it has already been loaded onto the system. Fig. 4 in the *Grawrock* patent also discloses this process whereby identifiers of the boot block, BIOS, BIOS extensions and OS loader are all provided to the TPM for recordation. This is so that a "challenger" may later determine whether the platform should behave in an expected manner for an intended purpose. Column 4, lines 36-40. The present invention verifies the authenticity of the BIOS <u>before</u> allowing it to be stored on the flash memory of the system. The difference between these two processes is like the difference between catching a criminal after the crime has been committed versus preventing the crime. As a result, the Examiner is relying upon an incorrect factual predicate in support of his rejection. That is, the Examiner has specifically asserted that *Grawrock* teaches that a TPM performs a signature verification of an update to the program. This is not true. *Grawrock* does not teach this. Thus, the combination of *Grawrock* and *Alexander* does not teach or suggest a TPM performing a signature verification of an update to a program, and then unlocking a memory unit using a TPM for storing the program if the signature verification of the update to the program is successful, and then modifying the program with the update to the program in response to the unlocking of the memory unit storing the program. At the most, the combination of *Alexander* and *Grawrock* would install an update to a program and then create identifiers of the update for recordation. Then, a "challenger" can later verify whether the program can be trusted. This is not the same as what is recited in the claims.

The claims specifically recite that the memory unit is unlocked after the verification is successful. According to the inventors, *Grawrock* already stores the updated program, and then performs a TPM verification. Thus, the prior art teaches away from the present invention.

As a result of the foregoing, Applicants respectfully assert that the claims are not obvious in view of the prior art.

Respectfully submitted,
WINSTEAD SECHREST & MINICK P.C.
Attorneys for Applicants

By: ____________________________
Kelly K. Kordzik
Reg. No. 36,571

P.O. Box 50784
Dallas, Texas 75201
(512) 370-2851

Austin_1\284612\1
7036-P177US 7/7/2005